AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Currently Amended): A ~~computer~~ system implemented on a computer apparatus for scanning a computer file including source code of a computer program in a given computer language for malware, the system comprising:

means for separating the source code into groups of constituent parts, each group comprising parts of a different type of structural part of the program;

means for processing each group to count the number of occurrences in that group of characters of a character set to obtain a frequency distribution of characters in that group;

means for comparing the character frequency distribution of each group with an expected range of frequency distributions; and

means for flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means.

Claim 2 (Previously Presented): A system according to claim 1, wherein the flagging means is operative to flag the file as suspect if the comparing means detects that the frequency distribution of one or more of said groups does not match an expected range.

Claim 3 (Previously Presented): A system according to claim 1, wherein the flagging means is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each group with an expected frequency distribution.

Claim 4 (Previously Presented): A system according to claim 1, wherein, in operation of the comparing means, the range of distributions considered as representing an acceptable match for the group is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

Claim 5 (Previously Presented): A system according to claim 1, further comprising:

means for maintaining an exception list of files which by their contents are to be treated as exceptions;

means for identifying a file as being included in the exception list; and

wherein a file is not marked as suspect if it is identified as being on the exception list.

Claim 6 (Previously Presented): A system according to claim 1, wherein duplicates of constituent parts are ignored.

Claim 7 (Previously Presented): A method for scanning a computer file including source code of a computer program in a given computer language for malware, the method comprising:

separating the source code into groups of constituent parts, each group comprising parts of a different type of structural part of the program;

processing each group to count the number of occurrences in that group of characters of a character set to obtain a frequency distribution of characters in that group;

comparing the character frequency distribution of each group with an expected range of frequency distributions; and

flagging the file as suspect or not depending on the result of one or more comparisons by the comparing.

Claim 8 (Previously Presented): A method according to claim 7, wherein the flagging is operative to flag the file as suspect if the comparing detects that the frequency distribution of one or more of said groups does not match an expected range.

Claim 9 (Previously Presented): A method according to claim 7, wherein the flagging is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each group with an expected frequency distribution.

Claim 10 (Previously Presented): A method according to claim 7, wherein, in the comparing, the range of distributions which is considered as representing an acceptable match for the group is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

Claim 11 (Previously Presented): A method according to claim 7, further comprising:

maintaining an exception list of files which by their contents are to be treated as exceptions;

identifying a file as being included in the exception list; and

wherein a file is not marked as suspect if it is identified as being on the exception list.

Claim 12 (Previously Presented): A system according to claim 1, wherein the groups comprise at least one of a group of comments, a group of variable names, a group of subroutine names, and a group of strings.

Claim 13 (Previously Presented): A method according to claim 7, wherein duplicates of constituent parts are ignored.

Claim 14 (Previously Presented): A method according to claim 7, wherein the groups comprise at least one of a group of comments, a group of variable names, a group of subroutine names, and a group of strings.

Claims 15 and 16 (Canceled).